IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re application of	:	**Confirmation No. 9646**
Kenji IWANO et al.	:	Attorney Docket No. 2002_0211A
Serial No.10/067,843	:	Group Art Unit 3626
Filed February 8, 2002	:	Examiner Dilek B. Cobanoglu
MEDICAL INFORMATION SYSTEM	:	**Mail Stop: Appeal Brief-PATENT**

APPEAL BRIEF FILED UNDER 37 CFR §41.37

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The following is Appellant's Brief, submitted under the provisions of 37 CFR § 41.37. Pursuant to the provisions of 37 CFR § 41.20(b)(2), the required fee of $540.00 is submitted concurrently herewith.

REAL PARTY IN INTEREST

The real party in interest is Panasonic Corporation of Osaka, Japan, the assignee of record (reel/frame 021897/0624).

RELATED APPEALS AND INTERFERENCES

There are no related appeals and interferences.

STATUS OF CLAIMS

Claim 2 is cancelled.

Claims 1 and 3-17 are rejected.

In a final Office Action of dated March 6, 2009, the Examiner rejected pending claims 1 and 3-17 in view of the prior art. The rejection of claims 1 and 3-17 is being appealed. A complete copy of all of the pending claims is provided in the attached Claims Appendix.

STATUS OF AMENDMENTS

No amendments were filed subsequent to the final Office Action dated March 6, 2009.

All previously filed amendments have been entered by the Examiner.

SUMMARY OF CLAIMED SUBJECT MATTER

A description of the subject matter of the rejected independent claims (i.e., claims 1, 8 and 9) is presented below. All references to the specification refer to the substitute specification filed on July 6, 2006.

Independent Claim 1

Independent claim 1 is directed to a medical information system (see entire medical information system illustrated in Fig. 1; and paragraphs [0009] and [0040] of the specification).

Claim 1 recites that the medical information system includes a patient server (see Fig. 1, reference element 1; and paragraph [0009], line 2 of the specification) comprising a first database (see Fig. 1, first database is a combination of reference elements 10f, 10g and 10h; and paragraph [0043], lines 6, 7 and 11-14 of the specification), said patient server 1 receiving vital information (see paragraph [0009], line 3 of the specification) and unique identifications allocated to patients (see Fig. 10; and paragraph [0073], lines 5-7 of the specification), storing and managing the received vital information and unique identifications in said first database such that the vital information is associated with a corresponding unique identification (see paragraphs [0009], line 3, and [0075], lines 1 and 2 of the specification), and such that correspondence between each of the unique identifications and patient data, wherein the patient data includes at least a patient name, is unrecognizable (see paragraph [0075], lines 1-5 of the specification), and transmitting the stored and managed vital information and unique identifications (see paragraph [0009], line 4 of the specification).

Claim 1 also recites that the medical information system includes a medical care provider

server connected to said patient server 1 through a first network (see Fig. 1, medical care provider server is illustrated as reference element 2, and first network is illustrated as reference element 3A; and paragraph [0009], lines 4 and 5 of the specification) and comprising a second database (see Fig. 1, second database is a combination of reference elements 11f, 11g and 11h; and paragraphs [0009], lines 5-8 and [0044], lines 5-10 of the specification), said medical care provider server 2 receiving the vital information and unique identifications from said first database of said patient server 1 through the first network 3A (see paragraph [0009], lines 5-8 of the specification), storing and managing the received vital information, unique identifications, and patient data in said second database (see paragraphs [0009], lines 5-8 and [0074], lines 3-6 of the specification), associate each of the unique identifications with corresponding patient data (see Fig. 11; and paragraph [0074], lines 3-6 of the specification), identifying corresponding patient data using each of the unique identifications, and allowing the stored and managed vital information, unique identifications, and patient data to be browsed (see paragraphs [0009], lines 7 and 8 of the specification).

In addition, claim 1 recites that the medical information system includes a patient terminal (see Fig. 1, reference element 4; and paragraph [0010], lines 1 and 2 of the specification) connected to said patient server 2 through a second network (see Fig. 1, second network illustrated as reference element 3B; and paragraph [0009], line 2 of the specification), said patient terminal 4 transmitting the vital information and unique identifications to said patient server 1 through the second network 3B (see paragraph [0009], lines 3 and 4 of the specification).

Moreover, claim 1 recites that the medical information system includes a doctor terminal

connected to said medical care provider 2 server through a third network (see Fig. 1, doctor terminal is illustrated as reference element 5, and third network is illustrated as reference element 3C; and paragraph [0009], lines 4-6 of the specification), said doctor terminal 5 browsing the vital information, unique identifications, and patient data stored and managed in said medical care provider server 2 through the third network (see paragraph [0009], lines 6-8 of the specification).

Claim 1 recites that the first network 3A is configured to allow communication between said patient server 1 and said medical care provider server 2 and disallow communication between either said patient terminal 4 or said doctor terminal 5 and either said patient server 1 or said medical care provider server 2, and disallow communication between said patient terminal 4 and said doctor terminal 5 (see Figs. 1 and 2; and paragraph [0079] of the specification).

Additionally, claim 1 recites that the second network 3B is configured to allow communication between said patient terminal 4 and said patient server 1, and disallow communication among said patient server 1, said medical care provider server 2, and said doctor terminal 5 (see Figs. 1 and 2; and paragraph [0079] of the specification).

Finally, claim 1 recites that the third network 3C is configured to allow communication between said doctor terminal 5 and said medical care provider server 2, and disallow communication among said patient server 1, said medical care provider server 2, and said patient terminal 4 (see Figs. 1 and 2; and paragraph [0079] of the specification).

Independent Claim 8

Independent claim 8 is directed to a medical information system (see entire medical

information system illustrated in Fig. 12; and paragraph [0020], lines 1 and 2 of the specification).

Claim 8 recites that the medical information system includes a plurality of patient servers (see Fig. 12, reference elements 1A-1Z; and paragraph [0020], line 2 of the specification) each comprising a first database (see paragraph [0083]; Fig. 1, first database is a combination of reference elements 10f, 10g and 10h; and paragraph [0043], lines 6, 7 and 11-14 of the specification) and each patient server 1A-1Z receiving vital information and unique identifications allocated to patients (see paragraphs [0083], [0020], lines 2-4, and [0073], lines 5-7 of the specification), storing and managing the received vital information and unique identifications in a respective first database such that the vital information is associated with a corresponding unique identification (see paragraphs [0083], [0020], line 3, and [0075], lines 1 and 2 of the specification), and such that correspondence between each of the unique identifications and patient data, wherein the patient data includes at least a patient name, is unrecognizable (see paragraphs [0083], and [0075], lines 1-5 of the specification), and transmitting the stored and managed vital information and unique identifications (see paragraphs [0083], and [0020] lines 3 and 4 of the specification).

In addition, claim 8 recites that the medical information system includes a medical care provider server connected to said plurality of patient servers 1A-1Z through a first network (see Fig. 12, medical care provider server illustrated as reference element 2, and first network is illustrated as reference element 3A; and paragraphs [0083] and [0020], lines 4-8 of the specification) and comprising a second database (see paragraph [0083]; Fig. 1, reference elements 11f, 11g and 11h; and paragraphs [0020], lines 4-8, and [0044], lines 5-10 of the

specification), said medical care provider server 2 receiving the vital information and unique identifications from each of said first databases of said plurality of patient servers 1A-1Z through the first network 3A (see paragraphs [0083] and [0020], lines 4-8 of the specification), storing and managing the received vital information, unique identifications, and patient data (see paragraph [0083] and [0020], lines 4-8 of the specification), associate each of the unique identifications with corresponding patient data (see paragraph [0083]; Fig. 11; and paragraph [0074], lines 3-6 of the specification), identifying the corresponding patient data using each of the unique identifications, and allowing the stored and managed vital information, unique identifications, and patient data to be browsed (see paragraphs [0083], and [0020], lines 4-8 of the specification).

Claim 8 also recites that the medical information system includes a plurality of patient terminals (see Fig. 12, reference element 4; and paragraph [0020], lines 8-11 of the specification) each connected to at least one of said patient servers 1A-1Z through a second network (see Fig. 12, reference element 3B; and paragraph [0020], lines 8-11 of the specification), said patient terminals 4 respectively transmit the vital information and unique identifications to said patient servers 1A-1Z through the second network 3B (see paragraph [0020], lines 8-11 of the specification).

Furthermore, claim 8 recites that a doctor terminal connected to said medical care provider server through a third network (see Fig. 12, doctor terminal is illustrated as reference element 5, and third network is illustrated as reference element 3C; and paragraph [0020], lines 11-14 of the specification), said doctor terminal 5 browsing the vital information, unique identifications, and patient data stored and managed in said medical care provider server 2

through the third network 3C (see paragraph [0020], lines 11-14 of the specification).

Claim 8 also recites that the first network 3A is configured to allow communication between said patient servers 1A-1Z and said medical care provider server 2 and disallow communication between either said patient terminals 4 or said doctor terminal 5 and either said patient servers 1A-1Z or said medical care provider server 2, and disallow communication between said patient terminals 4 and said doctor terminal 5 (see Fig. 12; and paragraphs [0083], and [0079] of the specification).

Moreover, claim 8 recites that the second network 3B is configured to allow communication between said patient terminals 4 and said patient servers 1A-1Z, and disallow communication among said patient servers 1A-1Z, said medical care provider server 2, and said doctor terminal 5 (see Fig. 12; and paragraphs [0083], and [0079] of the specification).

Finally, claim 8 recites that the third network 3C is configured to allow communication between said doctor terminal 5 and said medical care provider server 2, and disallow communication among said patient servers 1A-1Z, said medical care provider server 2, and said patient terminals 4 (see Fig. 12; and paragraphs [0083], and [0079] of the specification).

Independent Claim 9

Independent claim 9 is directed to a medical information system (see entire medical information system illustrated in Fig. 13; and paragraph [0022], line 1 of the specification).

Claim 9 recites that the medical information system includes a patient server (see paragraph [0086]; Fig 13, reference element 1; and paragraph [0022], lines 2-4 of the specification) comprising a first database (see paragraph [0086]; Fig 1, first database is a

combination of reference elements 10f, 10g and 10h; and paragraph [0043], lines 6, 7 and 11-14 of the specification), said patient server 1 receiving vital information and unique identifications allocated to patients (see paragraphs [0086], [0022], lines 2-4, and [0073], lines 5-7 of the specification), storing and managing the received vital information and said unique identifications such that the vital information is associated with a corresponding unique identification (see paragraphs [0086], [0022], lines 2-4, and [0075], lines 1 and 2 of the specification), and such that correspondence between each of the unique identifications and patient data, wherein the patient data includes at least a patient name, is unrecognizable (see paragraphs [0086] and [0075], lines 1-5 of the specification), and transmitting the stored and managed vital information and unique identifications (see paragraphs [0086], and [0022], lines 2-4 of the specification).

In addition, claim 9 recites that the medical information system includes a plurality of medical care provider servers connected to said patient server 1 through a first network (see paragraph [0086]; Fig 13, medical care provider servers are illustrated as reference elements 2A-2Z, and first network is illustrated as reference element 3A; and paragraph [0022], lines 4-8 of the specification) and each comprising a second database (see paragraph [0086]; Fig 1, second database is a combination of reference elements 11f, 11g and 11h; and paragraphs [0022], lines 4-8 and [0044], lines 5-10 of the specification), said medical care provider servers 2A-2Z respectively receiving the vital information and unique identifications from said patient server 1 through the first network 3A (see paragraphs [0086], and [0022], lines 4-8 of the specification), storing and managing the received vital information, unique identifications and patient data in said second database (see paragraphs [0086], and [0022], lines 4-8 of the specification), associate

each of the unique identifications with corresponding patient data (see paragraph [0086]; Fig 11; and paragraph [0074], lines 3-6 of the specification), identify corresponding patient data using each of the unique identifications, and allowing the stored and managed vital information, unique identifications, and patient data to be browsed (see paragraphs [0086], and [0022], lines 4-8 of the specification).

Further, claim 9 recites that the medical information system includes a patient terminal (see paragraph [0086]; Fig 13, reference element 4; and paragraph [0022], lines 8-11 of the specification) connected to said patient server 1 through a second network (see paragraph [0086]; Fig 13, reference element 3B; and paragraph [0022], lines 8-11 of the specification), said patient terminal 4 transmitting the vital information and unique identifications to said patient server 1 through the second network 3B (see paragraph [0022], lines 8-11 of the specification).

Claim 9 also recites that the medical information system includes a plurality of doctor terminals each connected to at least one of said medical care provider servers 2A-2Z through a third network (see paragraph [0086]; Fig 13, doctor terminals are illustrated as reference element 5, and third network is illustrated as reference element 3C; and paragraph [0022], lines 11-14 of the specification), said plurality of doctor terminals 5 browsing the vital information, unique identifications, and patient data stored and managed in said medical care provider servers 2A-2Z through the third network 3C, respectively (see paragraphs [0086], and [0022], lines 11-14 of the specification).

Moreover, claim 9 recites that the first network 3A is configured to allow communication between said patient server 1 and said medical care provider servers 2A-2Z and disallow communication between either said patient terminal 4 or said doctor terminals 5 and either said

patient server 1 or said medical care provider servers 2A-2A, and disallow communication between said patient terminal 4 and said doctor terminals 5 (see Fig 13; and paragraphs [0086], and [0079] of the specification).

Furthermore, claim 9 recites that the second network 3B is configured to allow communication between said patient terminal 4 and said patient server 1, and disallow communication among said patient server 1, said medical care provider servers 2A-2Z, and said doctor terminals 5 (see Fig 13; and paragraphs [0086], and [0079] of the specification).

Finally, claim 9 recites that the third network 3C is configured to allow communication between said doctor terminals 5 and said medical care provider servers 2A-2Z, and disallow communication among said patient server 1, said medical care provider servers 2A-2Z, and said patient terminal 4 (see Fig 13; and paragraphs [0086], and [0079] of the specification).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether claims 1 and 3-17 are unpatentable under 35 U.S.C. § 103(a) as being obvious in view of the combination of Joao (U.S. 6,283,761), Califano et al. (U.S. 2003/0039362) and Felsher (U.S. 2002/0010679).

ARGUMENT

Rejection Under 35 U.S.C. §103(a) Over the Combination of Joao (U.S. 6,283,761), Califano et al. (U.S. 2003/0039362) and Felsher (U.S. 2002/0010679)

Claims 1 and 3-17 were rejected under 35 U.S.C. §103(a) as being unpatentable over the combination of Joao (U.S. 6,283,761), Califano et al. (U.S. 2003/0039362) and Felsher (U.S. 2002/0010679). The Examiner's detailed rejections are set forth on pages 2-11 of the Final Office Action mailed on March 6, 2009.

Discussion of Joao (Primary) Reference

Joao discloses a medical information system including a server 10 that acts as a connection node for a health care provider device 20, a payer device 30, a patient device 40, and an intermediary device 50. The provider device 20, the payer device 30, the patient device 40, and/or intermediary device 50, can be any computer or communication device, including, but not limited to, a personal computer, a home computer, a server computer, a network computer, a hand held computer and the like. Server 10, provider device 20, payer device 30, patient device 40, and intermediary device 50, can transmit information to, as well as receive information from, any of the other devices 10, 20, 30, 40, and 50. Each of the devices 10, 20, 30, 40 and 50 are directly or indirectly linked with one another so as to facilitate direct or indirect bidirectional communication (see col. 14, lines 49-67 and col. 15, lines 1-17).

Specifically, Joao teaches that server 10 includes a database 10H that contains any and/or all of the information needed and/or required in order to perform any and/or all of the functions, services and/or operations of the medical information system. Database 10H contains data

and/or information regarding patient name, patient identification information, patient social security number or other identification information, data of birth, doctors or providers and so on. The data and/or information which is or which may be stored in the database 10H, can be utilized and/or can appear in any of the reports, diagnostic reports, treatment reports, evaluation reports, provider reports, payer reports, patient reports, training reports, and/or any reports created by the medical information system. The provider device 20, the payer device 30, the patient device 40 and the intermediary device 50, each contain, respectively, databases 20H, 30H, 40H, and 50H. Each of these databases can contain and/or be linked to any of the data and/or information described as being stored in the database 10H (see col. 16, lines 33-65).

While using the system of Joao, a user can enter information concerning the patient, the treatment, and or care, which is desired to be evaluated and or monitored. Server 10 uses database 10H to obtain patient information, patient medical history, family history, if pertinent, system information, provider information, and/or any other information which can be relevant and or pertinent (see col. 16, lines 33-65).

Based on the above discussion, it is apparent that the medical information system of Joao includes devices 10, 20, 30, 40 and 50 that are directly or indirectly linked with one another so as to facilitate direct or indirect bidirectional communication, such that the database 10H contains any and/or all of the information needed/used by the medical information system. Moreover, in view of the above, Joao teaches that the database 10H stores information regarding patient identifications (e.g., patient names) and associates these patient identifications with corresponding patient medical history.

The final Office Action of March 6, 2009 acknowledges Joao fails to disclose or suggest

that correspondence between each of the unique identification and patient data (including a patient name) is unrecognizable, as recited in independent claims 1, 8 and 9.

In light of the acknowledged deficiencies of Joao, the final Office action of March 6, 2009 relies on Califano for teaching the above-identified limitations of claims 1, 8 and 9 that are admittedly lacking from Joao.

Furthermore, the final Office Action of March 6, 2009 acknowledges that Joao fails to disclose or suggest the features of the second and third networks, as recited in independent claims 1, 8 and 9.

In light of the acknowledged deficiencies of Joao, the final Office action of March 6, 2009 relies on Felsher for teaching the features of the second and third networks recited in claims 1, 8 and 9 that are admittedly lacking from Joao.

Discussion of Califano (Secondary) Reference

Califano teaches that a patient's identity (i.e., patient's name) is stored in patient database 26 (see paragraph [0029], lines 1-4 and paragraph [0010]). Further, Califano teaches that a Virtual Private Identity (VPI) is generated as a unique identifier for the patient and stored in a VPI database 28 (see paragraph [0029], lines 4-6 and paragraph [0010]). In addition, Califano teaches that the database 28 stores an encrypted version of the patient's name in association with the generated VPI (i.e., unique identifier of the patient) (see paragraph [0029], lines 6-8). Califano also teaches that the patient's name is stored in the patient database 26 in association with the encrypted VPI (i.e., encrypted unique identifier of the patient) (see paragraph [0030], lines 8-12).

As a result, because the patient's name is stored in association with an encrypted version of the VPI (i.e., encrypted unique identifier of the patient) the relationship between the patient's name and the non-encrypted VPI (i.e., non-encrypted unique identifier of the patient) is difficult to recognize without a proper decryption key. However, since the patient's name is stored in association with the encrypted unique identifier of the patient, it is possible to obtain the relationship between the patient's name and the patient's non-encrypted unique identifier by simply applying a decryption key.

Discussion of Felsher (Secondary) Reference

Felsher discloses a system of maintaining security of medical records to prevent unauthorized access or use, and teaches that the system includes a medical information database 6 for storing patient medical records which may be encrypted or unencrypted. During operation, encrypted files are received and stored in conjunction with an index server 5 in the database 6. An index record is provided in the index server 5 for each database 6 entry, providing an identification for the patient, a locator for the associated record, and a set of access rules for the record. The patient records are intrinsically anonymous, and thus are identified only by association with the respective patient through index 5. Thus, database 6 maintains patient medical history records separate from corresponding patient identification information contained in the index server 5. Moreover, the patient records, albeit without the patient personally identifying the information contained therein, may be used for anonymous summary information searches.

Furthermore, the system of Felsher uses the internet as a preferred communications

network. Thus the records may be transmitted virtually anywhere on earth using a single infrastructure. Alternately, private networks or virtual private networks may be employed.

Claims 1 and 3-17

Independent claim 1 recites a medical information system including a patient server receiving, storing and managing vital information and unique identifications allocated to patients, such that the vital information is associated with a corresponding unique identification, and such that correspondence between each of the unique identifications and patient data (including at least a patient name) is unrecognizable. In addition, claim 1 recites that the medical information system includes a medical care provider server connected to the patient server through a first network, such that the medical care provider server receives the vital information and unique identifications from the patient server through the first network, stores/manages the received vital information, the received unique identifications, and patient data, and associates each of the unique identifications with corresponding patient data. Claim 1 also recites that the medical information system includes a patient terminal connected to the patient server through a second network, such that the patient terminal transmits the vital information and unique identifications to the patient server through the second network, and includes a doctor terminal connected to the medical care provider server through a third network, the doctor terminal browsing the vital information, unique identifications, and patient data stored and managed in the medical care provider server through the third network.

Regarding network communications between the patient server, the medical care provider server, the patient terminal, and the doctor terminal, claim 1 recites that: (i) the first network is

configured to allow communication between the patient server and the medical care provider server and disallow communication between either the patient terminal or the doctor terminal and either the patient server or the medical care provider server, and disallow communication between the patient terminal and the doctor terminal; (ii) the second network is configured to allow communication between the patient terminal and the patient server, and disallow communication among the patient server, the medical care provider server, and the doctor terminal; and (iii) the third network is configured to allow communication between the doctor terminal and the medical care provider server, and disallow communication among the patient server, the medical care provider server, and the patient terminal.

As discussed above, the medical system of Joao includes several devices that operate as a single entity without data restrictions. Specifically, Joao teaches that devices 10, 20, 30, 40 and 50 are directly or indirectly linked with one another so as to facilitate direct or indirect bidirectional communication, such that the database 10H contains any and/or all of the information needed.

Additionally, as mentioned above, Califano teaches that the encrypted virtual private identity (VPI) is generated in order to "mask" the patient's name.

Now, regarding a result of the combination of Joao and Califano, Applicants note that by combining the medical system of Joao with the encrypted VPI of Califano, the database 10H of Joao that stores all of the information and makes all of the information available to devices 10, 20, 30, 40 and 50 would make use of the encrypted VPI of Califano to "mask" the patient's name.

Thus, in view of the above, although the combination of Joao and Califano would result

in the database 10H storing all of the information to make all of the information available to devices 10, 20, 30, 40 and 50, while using the encrypted VPI to "mask" the relationship between patient's name and the patients unique identification, the combination of Joao and Califano still fails to disclose or suggest: (1) the patient server that manages the vital information and unique identifications and such that the correspondence between each of the unique identifications and patient data (including at least a patient name) is unrecognizable; (2) the medical care provider server connected to the patient server through the first network, such that the medical care provider server makes the vital data, unique identifications, and corresponding patient data (patient name) available; and (3) disallowing communication between the patient or doctor terminal and either the patient server or the medical care provider server.

Specifically, the combination of Joao and Califano would result in the relationship between the patient's name and the patient's unique identification always being masked by the encrypted VPI to all users/portions of the system, which fails to disclose or suggest that in the patient server the correspondence between each of the unique identifications patient data (patient's name) is unrecognizable and in the medical care provider server the correspondence between patient data (patient's name), the patient's unique ID and the vital information is available, and fails to disclose or suggest that the first network which provides communication between the patient server and the medical care provider server disallows communication between the patient or doctor terminal and either the patient server or the medical care provider server, as required by claim 1.

More specifically, claim 1 requires the medical care provider server to make the patient's name available (i.e., the patient's name is not masked) and requires the patient server to make

the correspondence between the patient's name and the unique identification to be unrecognizable, whereas the combination of Joao and Califano would require the relationship between the patient's name and the patient's ID to be masked to all parts of the medical system.

Now, turning to the differences between the Califano reference and the claimed limitation that a correspondence between each of the unique identifications and patient data (including the patient's name) is unrecognizable, it is noted that Califano teaches that the patient's name is stored in association with the encrypted VPI related to the unique identifier of the patient, making it is possible to obtain the relationship between the patient's name and the patient's unique identifier by simply applying a decryption key to the VPI.

Therefore, it is clear that the structure of the relationship between the patient's name, the unique identifier of the patient, and the VPI, as disclosed by Califano, fails to disclose or suggest the patient server receiving, storing and managing vital information and unique identifications allocated to patients, such that the vital information is associated with a corresponding unique identification, and such that correspondence between each of the unique identifications and patient data (including at least a patient name) is unrecognizable, as required by claim 1.

In other words, Califano teaches that the relationship between the patient's name and the patient's unique identifier is available using decryption, which is not the same as the correspondence between each of the unique identifications and patient data (including at least a patient name) being unrecognizable to the patient server, as required by claim 1.

The feature of the correspondence between the unique identifications and the patient data being unrecognizable is described in paragraph [0075] of the specification of the present invention, which states "although the patient server 1 stores the vital data for each of the ID's,

the patient server 1 does not store the patient data corresponding to each of the IDs. Accordingly if the patient server 1 were accessed without authorization, it would be impossible to identify each of the vital data of a particular patient."

Therefore, since according to Califano the relationship between the patient's name and the patient's ID can be accessed using decryption (i.e., is recognizable), Califano cannot be relied upon for disclosing or suggesting that from the patient server the correspondence between each of the unique identifications and patient data (including at least a patient name) is unrecognizable (i.e., impossible to identify), as required by claim 1.

Now, turning to the differences between the Felsher reference and the claimed first network, second network, and third network, as recited in claim 1, it is respectfully submitted that Felsher, as a whole, is not suggestive of the presently claimed invention. Specifically, Applicants respectfully submit that Felsher teaches away from the invention Joao, and as such, supports the non-obviousness of the claimed invention. More specifically, in contrast to Joao, Felsher clearly describes a medical security system including a database 6 that maintains patient medical history records separate from corresponding patient identification information contained in the index server 5.

By virtue of maintaining the database 6 separate from the index server 5, Felsher teaches against associating patient medical records with the corresponding unique identification, as required by Joao.

Moreover, because Felsher does not also employ a system that maintains patient medical history that is associated with corresponding unique identification information in a same database, it is incompatible with Joao. Substituting the medical security system of Felsher for

the health care information system of Joao, renders the system of Joao unsatisfactory for its intended purpose because a user cannot then access a patient's medical history and/or other information that can be relevant and/or pertinent using corresponding unique identifications. Because the proposed modification/substitution changes the principle of operation of Joao and renders Joao unsatisfactory for its intended purpose, Felsher is incompatible with Joao. Thus, considering the references as a whole, there is no reason to make the proposed combination of references. As a result, claim 1 is patentable over the combination of Joao, Califano and Felsher.

As discussed in the January 31, 2008 Amendment, MPEP § 2145(III) establishes that a claimed combination cannot change the principle of operation of the primary reference or render the reference inoperable for its intended purpose, and MPEP § 2145(VI) establishes that a prior art reference must be considered in its entirety. The Applicants respectfully submit that, although Felsher is in the same field of endeavor as Joao, the Examiner has not considered Felsher in its entirety. Specifically, it does not appear that the Examiner has considered that maintaining the database 6 separate from the index server 5, teaches against associating patient medical records with the corresponding unique identification, as required by Joao. Thus, as discussed above, when Felsher is considered in its entirety, the structure required by Felsher teaches away from the structure required by Joao, because the structure required by Felsher would change the principle of operation of Joao and render Joao inoperable for its intended purpose.

Furthermore, Applicants submit that the combination of Joao, Califano and Flesher fail to disclose or suggest the features required by the structure of the first, second and third networks, as recited in claim 1.

Therefore, because of the above-mentioned distinctions it is believed clear that claim 1 and claims 3-7 that depend therefrom would not have been obvious or result from any combination of Joao, Califano and Felsher.

Independent claim 8 recites the same distinguishing limitations discussed above regarding claim 1. Therefore, claim 8 is patentable over the Joao, Califano and Felsher references for reasons similar to those set forth above regarding claim 1.

Specifically, claim 8 recites a medical information system including, in part, a plurality of patients servers each including a first database where each patient server receives vital information and unique identifications allocated to patients, stores and manages the received vital information and unique identifications in a respective first database such that the vital information is associated with a corresponding unique identification, and such that correspondence between each of the unique identifications and patient data, wherein the patient data includes at least a patient name, is unrecognizable.

Moreover, the medical system of claim 8 includes a first network configured to allow communication between the patient servers and a medical care provider server and disallow communication between either patient terminals or a doctor terminal and either the patient servers or the medical care provider server, and disallow communication between the patient terminals and the doctor terminal.

Furthermore, the medical system of claim 8 includes a second network configured to allow communication between the patient terminals and the patient servers, and disallow communication among the patient servers, the medical care provider server, and the doctor terminal. The medical system of claim 8 also includes a third network configured to allow

communication between the doctor terminal and the medical care provider server, and disallow communication among the patient servers, the medical care provider server, and the patient terminals.

Independent claim 9 recites the same distinguishing limitations discussed above regarding claim 1. Therefore, claim 9 is patentable over the combination of Joao, Califano and Felsher for reasons similar to those set forth above regarding claim 1.

Specifically, claim 9, recites a medical information system including, in part, a patient server comprising a first database, where the patient server receives vital information and unique identifications allocated to patients, stores and manages the received vital information and said unique identifications such that the vital information is associated with a corresponding unique identification and such that correspondence between each of the unique identifications and patient data, wherein the patient data includes at least a patient name, is unrecognizable.

Moreover, the medical information system of claim 9 includes a first network configured to allow communication between the patient server and medical care provider servers and disallow communication between either a patient terminal or doctor terminals and either the patient server or the medical care provider servers, and disallow communication between the patient terminal and the doctor terminals.

Furthermore, the medical system of claim 9 includes a second network configured to allow communication between the patient terminal and the patient server, and disallow communication among the patient server, the medical care provider servers, and the doctor terminals. The medical information system of claim 9 also includes a third network configured to allow communication between the doctor terminals and the medical care provider servers, and

disallow communication among the patient server, the medical care provider servers, and the patient terminal.

Conclusion

In view of the above, it is respectfully submitted that independent claims 1, 8 and 9 and claims 3-7, 10-13 and 14-17 which depend therefrom would not have been obvious or result from any combination of Joao, Califano and Felsher. Furthermore, there is no disclosure or suggestion in Joao, Califano and/or Felsher or elsewhere in the prior art of record which would have caused a person of ordinary skill in the art to modify Joao, Califano and/or Felsher to obtain the invention of independent claim 1, 8 and 9. Accordingly, the Examiner's decision to finally rejection claims 1 and 2-17 should be reversed.

Respectfully submitted,

Kenji Iwano, et al.

By: /Andrew L. Dunlap/
2009.08.10 16:49:51 -04'00'

Andrew L. Dunlap
Registration No. 60,554
Attorney for Applicants

ALD/led
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
August 10, 2009

CLAIMS APPENDIX

Claim 1 A medical information system comprising:

a patient server comprising a first database, said patient server receiving vital information and unique identifications allocated to patients, storing and managing the received vital information and unique identifications in said first database such that the vital information is associated with a corresponding unique identification, and such that correspondence between each of the unique identifications and patient data, wherein the patient data includes at least a patient name, is unrecognizable, and transmitting the stored and managed vital information and unique identifications;

a medical care provider server connected to said patient server through a first network and comprising a second database, said medical care provider server receiving the vital information and unique identifications from said first database of said patient server through the first network, storing and managing the received vital information, unique identifications, and patient data in said second database, associate each of the unique identifications with corresponding patient data, identifying corresponding patient data using each of the unique identifications, and allowing the stored and managed vital information, unique identifications, and patient data to be browsed;

a patient terminal connected to said patient server through a second network, said patient terminal transmitting the vital information and unique identifications to said patient server through the second network; and

a doctor terminal connected to said medical care provider server through a third network, said doctor terminal browsing the vital information, unique identifications, and patient data

stored and managed in said medical care provider server through the third network,

wherein the first network is configured to allow communication between said patient server and said medical care provider server and disallow communication between either said patient terminal or said doctor terminal and either said patient server or said medical care provider server, and disallow communication between said patient terminal and said doctor terminal,

wherein the second network is configured to allow communication between said patient terminal and said patient server, and disallow communication among said patient server, said medical care provider server, and said doctor terminal, and

wherein the third network is configured to allow communication between said doctor terminal and said medical care provider server, and disallow communication among said patient server, said medical care provider server, and said patient terminal.

Claim 2 (Cancelled)

Claim 3 A medical information system according to claim 1, further comprising a sensor for measuring vital data, wherein the vital information includes a measurement value by said sensor.

Claim 4 A medical information system according to claim 1, wherein:

said doctor terminal transmits, as consultation data, an inquiry regarding a health status of a patient to said medical care provider server through the third network; and

the vital information transmitted from said patient terminal to said patient server through the second network includes a reply to the inquiry transmitted to said patient terminal.

Claim 5 A medical information system according to claim 1, further comprising:

a first unauthorized access prevention section provided in the first network;

a second unauthorized access prevention section provided in the second network; and

a third unauthorized access prevention section provided in the third network,

wherein said first and third unauthorized access prevention sections have higher security levels than a security level of said second unauthorized access prevention section.

Claim 6 A medical information system according to claim 5, wherein:

said first unauthorized access prevention section comprises a firewall and a virtual private network;

said second unauthorized access prevention section comprises a remote access server; and

said third unauthorized access prevention section comprises a terminal authentication server.

Claim 7 A medical information system according to claim 1, wherein said patient server and said medical care provider server are respectively clustered.

Claim 8 A medical information system comprising:

a plurality of patient servers each comprising a first database and each patient server receiving vital information and unique identifications allocated to patients, storing and managing the received vital information and unique identifications in a respective first database such that the vital information is associated with a corresponding unique identification, and such that correspondence between each of the unique identifications and patient data, wherein the patient data includes at least a patient name, is unrecognizable, and transmitting the stored and managed vital information and unique identifications;

a medical care provider server connected to said plurality of patient servers through a first network and comprising a second database, said medical care provider server receiving the vital information and unique identifications from each of said first databases of said plurality of patient servers through the first network, storing and managing the received vital information, unique identifications, and patient data, associate each of the unique identifications with corresponding patient data, identifying the corresponding patient data using each of the unique identifications, and allowing the stored and managed vital information, unique identifications, and patient data to be browsed;

a plurality of patient terminals each connected to at least one of said patient servers through a second network, said patient terminals respectively transmit the vital information and unique identifications to said patient servers through the second network; and

a doctor terminal connected to said medical care provider server through a third network, said doctor terminal browsing the vital information, unique identifications, and patient data stored and managed in said medical care provider server through the third network,

wherein the first network is configured to allow communication between said patient

servers and said medical care provider server and disallow communication between either said patient terminals or said doctor terminal and either said patient servers or said medical care provider server, and disallow communication between said patient terminals and said doctor terminal,

wherein the second network is configured to allow communication between said patient terminals and said patient servers, and disallow communication among said patient servers, said medical care provider server, and said doctor terminal, and

wherein the third network is configured to allow communication between said doctor terminal and said medical care provider server, and disallow communication among said patient servers, said medical care provider server, and said patient terminals.

Claim 9 A medical information system comprising:

a patient server comprising a first database, said patient server receiving vital information and unique identifications allocated to patients, storing and managing the received vital information and said unique identifications such that the vital information is associated with a corresponding unique identification, and such that correspondence between each of the unique identifications and patient data, wherein the patient data includes at least a patient name, is unrecognizable, and transmitting the stored and managed vital information and unique identifications;

a plurality of medical care provider servers connected to said patient server through a first network and each comprising a second database, said medical care provider servers respectively receiving the vital information and unique identifications from said patient server

through the first network, storing and managing the received vital information, unique identifications and patient data in said second database, associate each of the unique identifications with corresponding patient data, identify corresponding patient data using each of the unique identifications, and allowing the stored and managed vital information, unique identifications, and patient data to be browsed;

a patient terminal connected to said patient server through a second network, said patient terminal transmitting the vital information and unique identifications to said patient server through the second network; and

a plurality of doctor terminals each connected to at least one of said medical care provider servers through a third network, said plurality of doctor terminals browsing the vital information, unique identifications, and patient data stored and managed in said medical care provider servers through the third network, respectively,

wherein the first network is configured to allow communication between said patient server and said medical care provider servers and disallow communication between either said patient terminal or said doctor terminals and either said patient server or said medical care provider servers, and disallow communication between said patient terminal and said doctor terminals,

wherein the second network is configured to allow communication between said patient terminal and said patient server, and disallow communication among said patient server, said medical care provider servers, and said doctor terminals, and

wherein the third network is configured to allow communication between said doctor terminals and said medical care provider servers, and disallow communication among said

patient server, said medical care provider servers, and said patient terminal.

Claim 10 A medical information system according to claim 8, wherein each of said plurality of patient terminals includes a sensor for measuring vital data, and the vital information includes a measurement value by said sensor.

Claim 11 A medical information system according to claim 8, wherein:

said doctor terminal transmits, as consultation data, an inquiry regarding a health status of a patient to said medical care provider server through the third network; and

the vital information transmitted from one of said patient terminals to a corresponding patient server through the second network includes a reply to the inquiry transmitted to said one of said patient terminals.

Claim 12 A medical information system according to claim 8, further comprising:

a first unauthorized access prevention section provided in the first network;

a second unauthorized access prevention section provided in the second network; and

a third unauthorized access prevention section provided in the third network,

wherein said first and third unauthorized access prevention sections have higher security levels than a security level of said second unauthorized access prevention section.

Claim 13 A medical information system according to claim 12, wherein:

said first unauthorized access prevention section comprises a firewall and a virtual

private network;

said second unauthorized access prevention section comprises a remote access server; and

said third unauthorized access prevention section comprises a terminal authentication server.

Claim 14 A medical information system according to claim 9, wherein said patient terminal includes a sensor for measuring vital data, and the vital information includes a measurement value by said sensor.

Claim 15 A medical information system according to claim 9, wherein:

each of said plurality of doctor terminals transmits, as consultation data, an inquiry regarding a health status of a patient through the third network to a respective one of said plurality of medical care provider servers; and

the vital information transmitted from said patient terminal to said patient server through the second network includes a reply to the inquiry transmitted to said patient terminal.

Claim 16 A medical information system according to claim 9, further comprising:

a first unauthorized access prevention section provided in the first network;

a second unauthorized access prevention section provided in the second network; and

a third unauthorized access prevention section provided in the third network,

wherein said first and third unauthorized access prevention sections have higher security

levels than a security level of said second unauthorized access prevention section.

Claim 17 A medical information system according to claim 16, wherein:

said first unauthorized access prevention section comprises a firewall and a virtual private network;

said second unauthorized access prevention section comprises a remote access server; and

said third unauthorized access prevention section comprises a terminal authentication server.

EVIDENCE APPENDIX

None

RELATED PROCEEDINGS

None